



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,157	09/06/2001	Osamu Shibata	NAKI-BP89	9192

21611 7590 08/09/2006

SNELL & WILMER LLP  
600 ANTON BOULEVARD  
SUITE 1400  
COSTA MESA, CA 92626

EXAMINER
----------

MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 08/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	09/936,157		SHIBATA ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Aravind K. Moorthy		2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 28 April 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-12 and 17-31 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 and 17-31 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 September 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                                    |

**DETAILED ACTION**

1. This is in response to the amendment filed on 28 April 2006.
2. Claims 1-12 and 17-31 are pending in the application.
3. Claims 13-16 have been cancelled.
4. Claims 1-12 and 17-31 are rejected.

***Response to Arguments***

5. Applicant's arguments with respect to claims 1-12 and 17-20 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-12 and 17-31 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

For independent claims 1, 11, 12, 17, 19 and 21-23, the claims have been amended to include the limitation "the scrambled access information being used by the access device and the storage medium for calculating the first and second response values, respectively". However, after a review of the specification, the examiner finds no support for this limitation. If the

Art Unit: 2131

applicant finds this to be an error, the examiner invites the applicant to point out in the specification where this limitation has support.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**7. Claims 1-3, 8-12, and 17-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al U.S. Patent No. 6,289,455 B1 in view of Hellman U.S. Patent No. 5,872,917.**

As to claims 1, 11, 12, 17, 19 and 21-23, Kocher et al discloses an authentication communication system which includes (a) a storage medium having an area for storing digital information and (b) an access device for reading/writing digital information from/into the area, the authentication communication system comprising:

a first authentication phase in which the access device transmits to the storage medium scrambled access information generated by scrambling access information which shows the area [column 19, lines 36-43];

a second authentication phase in which the storage medium authenticates whether the access device is authorized [column 19 line 50 to column 20 line 41];  
and

a transfer phase in which, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts

the access information from the scrambled access information that was used in the authentication protocol, and the access device reads/writes digital information from/into the area shown by the access information [column 26 line 45 to column 27 line 32].

Kocher et al does not teach that the storage medium is authenticated by a challenge-response authentication protocol [column 3, lines 48-55]. Kocher et al does not teach that first and second response values are compared.

Hellman teaches the challenge-response authentication protocol and its benefits [column 6 line 57 to column 8 line 5]. Hellman teaches that a first and second response is compared [column 6 line 57 to column 8 line 5].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kocher et al so that the storage medium would have been authenticated using a challenge-response authentication protocol using the scrambled access information. The scrambled access information would have been used to calculate first and second response values. The first and second response values would have been compared to authenticate the challenge-response protocol.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kocher et al by the teaching of Hellman because the security of the authentication, based on the addition of PAD, is improved even when relatively short passwords are used. The likelihood of successful dictionary attacks is also reduced because the number of eavesdropper computations needed to search a set of probable passwords (e.g.,

names) is increased significantly. However, no additional time is needed for the user to generate his response or to validate the host's response [column 5, lines 47-59].

As to claims 2 and 18, Kocher et al teaches an access information acquisition unit for acquiring the access information that shows the area [column 11, lines 33-65]. Kocher et al teaches a random number acquisition unit for acquiring a random number [column 14, lines 32-42]. Kocher et al teaches a generation unit for generating random number access information by combining the access information and the random number [column 14, lines 32-42]. Kocher et al teaches an encryption unit for encrypting the random number access information according to an encryption algorithm, to generate the scrambled access information, the storage medium includes a response value generation unit for generating a response value from the scrambled access information, and the access device includes an authentication unit for authenticating whether the storage medium is authorized using the response value [column 11, lines 33-65].

As to claims 3 and 20, Kocher et al teaches a decryption unit for decrypting the scrambled access information according to a decryption algorithm to obtain the random number access information. Kocher et al teaches a separation unit for separating the access information from the random number access information [column 11, lines 33-65].

As to claim 8, Kocher et al teaches that in the transfer phase, the storage medium, which stores digital information in the area, includes an encryption unit for reading the digital information from the area shown by the access information and encrypting the digital information according to an encryption algorithm to generate encrypted digital information [column 22, lines 35-55], and the access device, which reads the digital information from the area, includes a decryption unit for decrypting the encrypted digital information according to a

Art Unit: 2131

decryption algorithm to obtain the digital information, the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm [column 22, lines 35-55].

As to claim 9, Kocher et al teaches a digital information acquisition unit for acquiring the digital information. Kocher et al teaches an encryption unit for encrypting the digital information according to an encryption algorithm to generate encrypted digital information [column 22, lines 35-55]. Kocher et al teaches that the storage medium includes a decryption unit for decrypting the encrypted digital information according to a decryption algorithm to obtain the digital information [column 22, lines 35-55]. Kocher et al teaches writing the digital information into the area shown by the access information. Kocher et al teaches the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm [column 22, lines 35-55].

As to claim 10, Kocher et al teaches a digital information acquisition unit for acquiring the digital information, as discussed above. Kocher et al teaches a content key acquisition unit for acquiring a content key [column 22, lines 35-55]. Kocher et al teaches a first encryption unit for encrypting the acquired content key according to a first encryption algorithm to generate an encrypted content key [column 22, lines 35-55]. Kocher et al teaches a second encryption unit for encrypting the encrypted content key according to a second encryption algorithm to generate a double- encrypted content key [column 22, lines 35-55]. Kocher et al teaches and a third encryption unit for encrypting the digital information according to a second encryption algorithm using the content key, to generate encrypted digital information [column 22, lines 35-55]. Kocher et al teaches that the storage medium includes a decryption unit for decrypting the double

Art Unit: 2131

encrypted content key according to a first decryption algorithm to obtain the encrypted content key, and writing the encrypted content key into the area shown by the access information, and the storage medium further includes an area for storing the encrypted digital information [column 22, lines 35-55].

**8. Claims 4-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al U.S. Patent No. 6,289,455 B1 and Hellman U.S. Patent No. 5,872,917 as applied to claim 1 above, and further in view of Vobach U.S. Patent No. 5,193,115.**

As to claim 4, the Kocher-Hellman combination does not teach that in the first authentication phase, the access device further includes a random number seed storage unit for storing a random number seed, and the random number acquisition unit acquires the random number by reading the random number seed from the random number seed storage unit.

Vobach teaches a random number seed storage unit for storing a random number seed, and the random number acquisition unit acquires the random number by reading the random number seed from the random number seed storage unit [column 9, lines 21-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Kocher-Hellman combination so that the random number are created with a random number seed that is stored in a storage unit. The random numbers would have been acquired from the storage unit.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Kocher-Hellman combination by the teaching of Vobach because the masking tape string only appears to an eavesdropper as a summand of the known ciphertext string, reconstructing it depends upon knowing the plaintext message string.



Art Unit: 2131

Since, for a given encrypted message, there will be many equally probably possible plaintext message strings, there will be as many equally probable possible masking tape strings. In short, the plaintext message string "masks" the masking tape string [column 6 line 64 to column 7 line 8].

As to claim 5, the combination of the Kocher-Hellman combination and Vobach teaches that in the first authentication phase, the access device further writes the scrambled access information over the random number seed stored in the random number seed storage unit, as a new random number seed [Vobach column 9, lines 40-63].

As to claim 6, the combination of the Kocher-Hellman combination and Vobach teaches that in the first authentication phase, the access device further includes a random number seed storage unit for storing a random number seed, and the random number acquisition unit acquires the random number, by reading the random number seed from the random number seed storage unit and generating the random number based on the random number seed [Vobach column 9, lines 21-63].

As to claim 7, the combination of the Kocher-Hellman combination and Vobach teaches that in the first authentication phase, the access device further writes the random number over the random number seed stored in the random number seed storage unit as a new random number seed, as discussed above.

Art Unit: 2131

**9. Claims 24-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al U.S. Patent No. 6,289,455 B1 and Hellman U.S. Patent No. 5,872,917 as applied to claims 1, 11, 12, 17, 19 and 21-23 above, and further in view of Mann U.S. Patent No. 6,374,399 B1.**

As to claims 24-31, the Kocher-Hellman combination teaches that access information comprises address information, as discussed above.

The Kocher-Hellman combination does not teach that access information comprises data size information.

Mann teaches access information that comprises data size information [column 11, lines 22-26].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Kocher-Hellman combination so that the access information would have included address information as well as data size information.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Kocher-Hellman combination by the teaching of Mann because it lets the target device know how much space to a lot for the data during the write function [column 1, lines 51-67].

*Conclusion*

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy   
August 7, 2006

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100